RSAC 2025 Conference

Many Voices.
One Community.

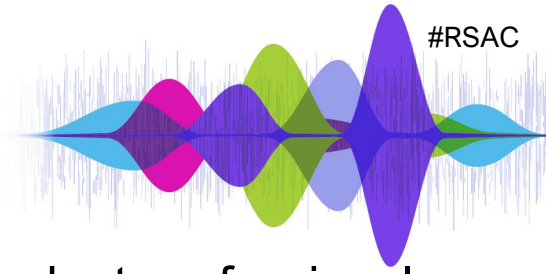
SESSION ID: SAT – M02

Untangle This Ball of Fuzz – Leveraging Insights on Cyber System Complexity

Brett Tucker

Brett Tucker PMP, CSSBB, CISSP, CGRC
Technical Manager, Cyber Risk Management
Carnegie Mellon University Software Engineering Institute

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Disclaimer

Copyright statement and disclaimers for presentation content:

Copyright 2025 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

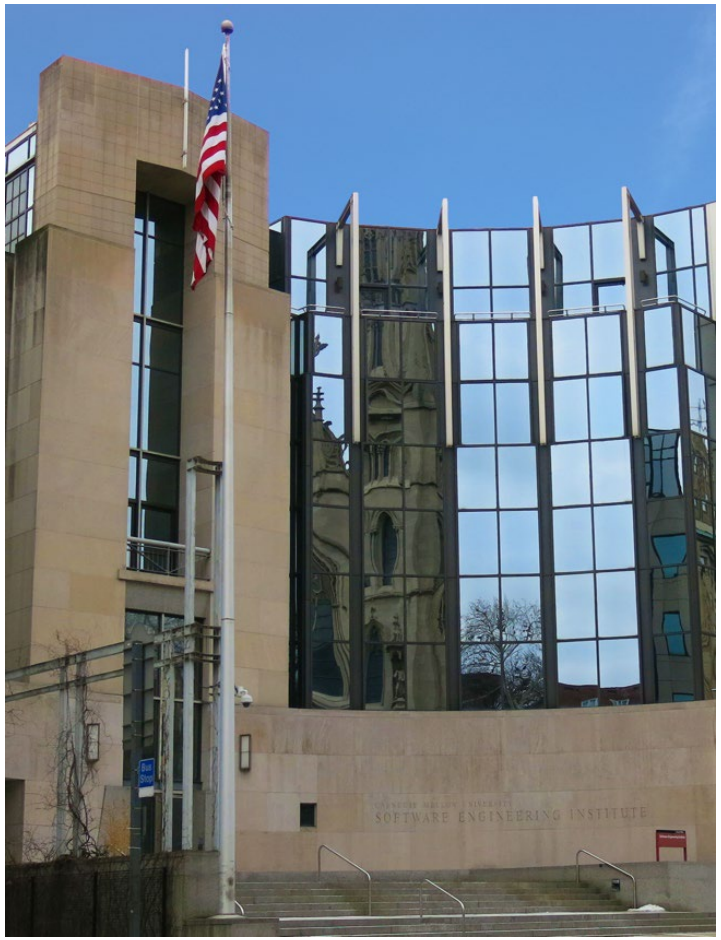
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM25-0347

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CMU Software Engineering Institute (SEI)



Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD.
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

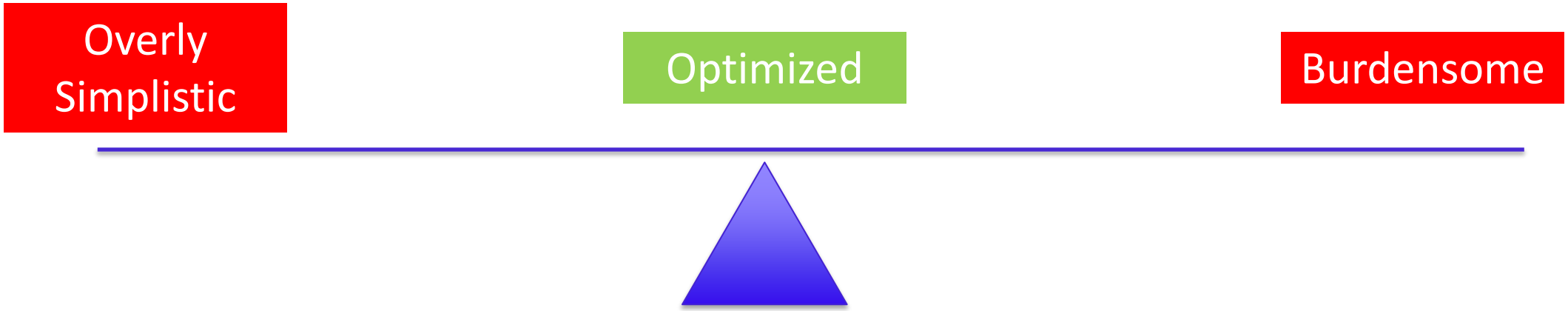
Value Proposition in Understanding Complexity

- **Not Easy:** Organizations must strive to make better risk-based decisions.
- **Security is Complex:** Threat actor tactics and techniques continually shift.
- **Measurement May Help:** The complexity of the system may inhibit or enhance performance.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Can Complexity of Cyber Be Measured?

- **Complexity:**
  - The state of having many parts and being difficult to understand.
  - We want to reduce the complexity of cybersecurity that inhibits strategic objectives.
- Hypothesis - Complexity is a range…



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Use Case Example – Why Measure Complexity?

- Imagine having a speedometer for your cybersecurity control stack.
  - Provides indication of activity of your system.
  - Could be thought of as a proxy for risk.
    - High speed = high risk
    - Low speed = high risk

- Changes to assets and controls could impact the index.
  - Think about physical, administrative, and technical controls.
  - Dynamic environments that have many devices coming and going.

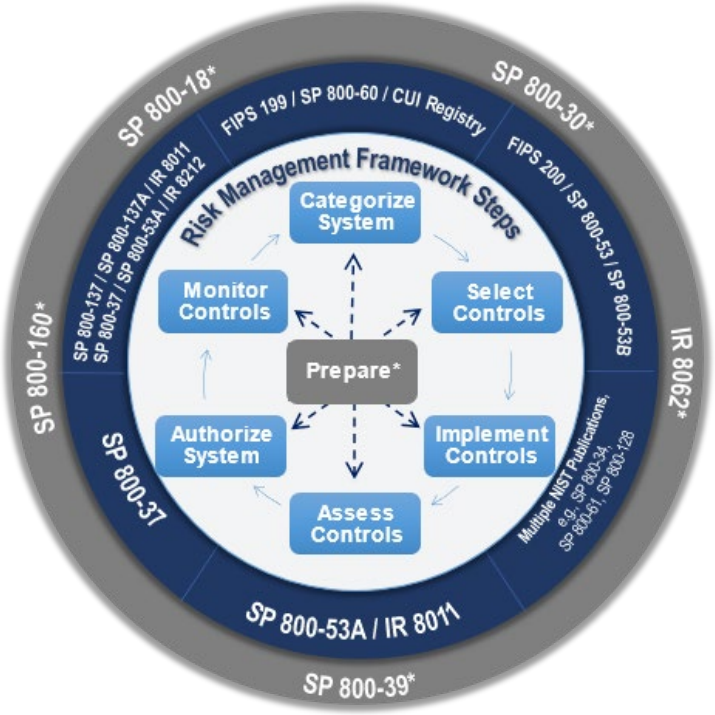
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Use Case Example of How to Use a Complexity Index

- NIST SP 800-37 Rev 2
  - Risk Management Framework

- Authorizing officials may not understand the risks they are taking.

- Complexity enables sensitivity analysis for system changes.



Source: NIST Website - Risk Management | CSRC

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Decomposing Cybersecurity Complexity

The cybersecurity stack of any organization has many diverse elements.

These elements may be contributing in part or in tandem to create a complex ecosystem.

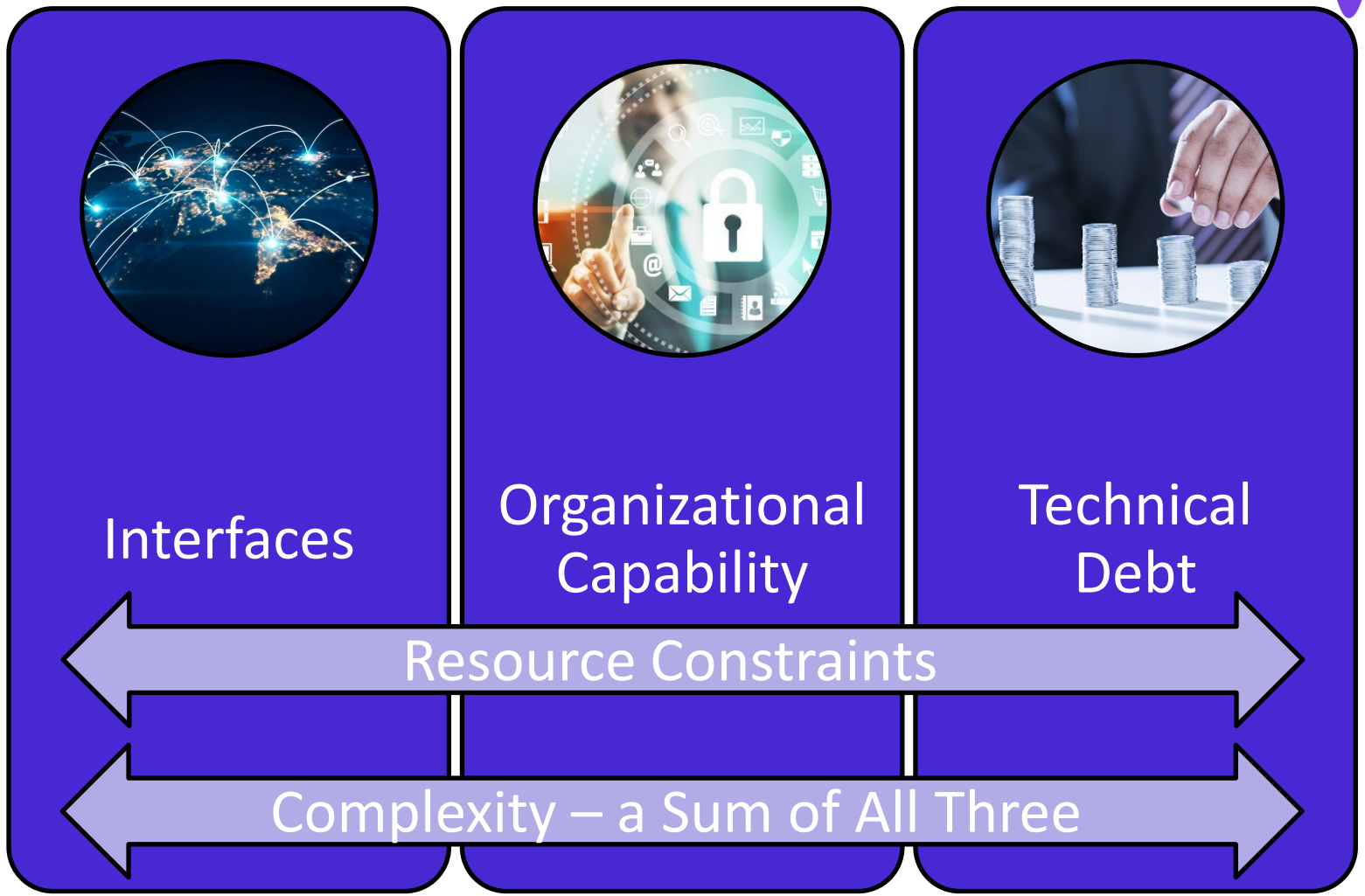
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Additional Elements to Consider

Other elements may be “cross-cutting”.

Cross-cutting considerations include:

- Supply Chain
- Resource Constraints



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Quantifying System Interfaces – WHERE WE STARTED…

Interfaces

Complexity may be related to the number of interconnections in a system – technical or administrative

May be quantified for the index using **Metcalfe's Law**.

- Communication Channels = N^2

This research also considered net flow for a period of time.

- Sensor selection and placement critical
- May simplify by limiting to internal flow

References: What is Metcalfe's Law? Definition, Types & Examples Techopedia, https://www.techopedia.com/definition/29066/metcalfes-law

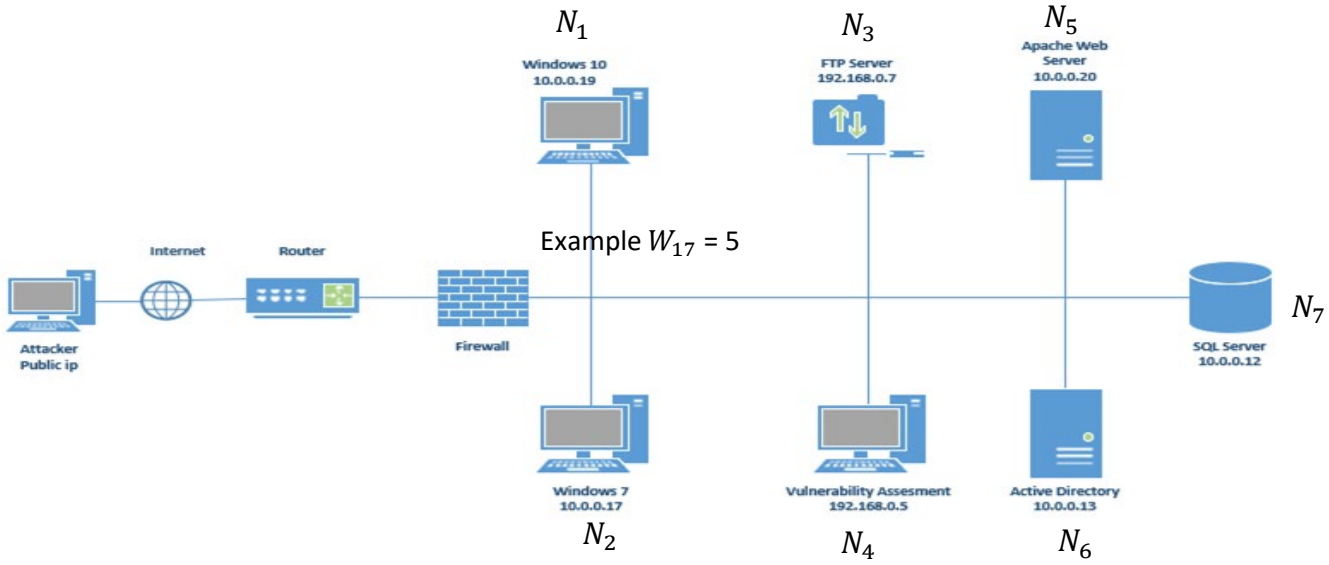
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Evolution of Network Quantification Research – WHERE WE ARE…

Metcalfe's Law may need more…

Graph Theory considered for greater fidelity.

Assume the following network:



First Determine:
Nodes Behind Firewall = 7
Potential Edges = 64
Weights could be assigned and averaged

Next Consider:
Sensitivity analysis related to adding new nodes.

Edges increase, and the weighting of the connections may shift.

We are concerned about the delta in the shift…

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Quantifying Organizational Capability

Organizational Capability

Complexity may be related to the ability of the organization to manage and utilize its assets effectively.

- Represented by workforce skills and capabilities.

This complexity factor may be measured by analyzing the structure of the organization and needs as they relate to the security stack.

- National Initiative for Cybersecurity Education (NICE) The National Cybersecurity Workforce Framework Version 1.0

Scores may be determined by organizational needs.

Assume:
Organizational current needs = 45 distinct skills
New skills needed given addition of a new asset = 3

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Quantifying Technical Debt

Technical Debt

Complexity may also depend upon technical debt.

- Size and potential errors in the code base.
- Architectural inadequacies.
- Legacy infrastructure.

Technical debt is challenging to measure.

Some research shows that the following may be considered for quantification:

- Heuristics related to errors per lines of code

References: Li, Malaiya, and Denton - https://www.cs.colostate.edu/pubserv/pubs/Li-malaiya-p-li98.pdf

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Technical Debt – Evolution of Understanding

Technical debt translates to financial impacts of mitigating vulnerabilities and capital improvements.

Some measurement(s) may be contextually dependent.

Li, Malaiya, & Denton showed ~0.5% Errors per Lines of Code

Example: Expect ~30 Errors for 6000 Lines of Code

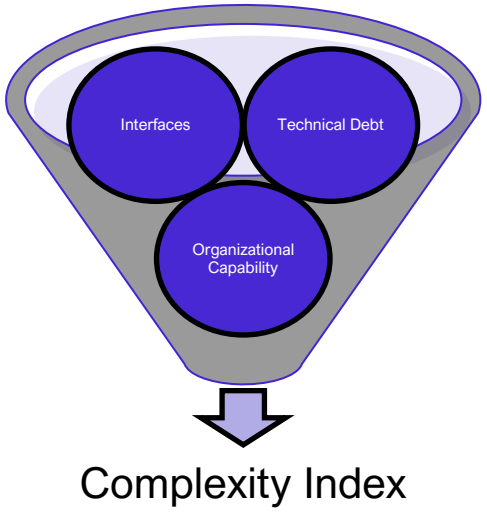
New software includes ~6,000,000 of code = ~30000 Errors

How much does this cost considering not all errors equate to vulnerabilities?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Index Will Come from an Integration of Parts

- The three elements will each yield a quantitative measure.
  - Additional research needed to determine the validity of the math.



$$S_i = \sum_{j=1}^{n} S_{ij} W_j$$

- $S_i = Complexity\ Index\ for$ "i" elements
- $S_{ij} = the\ score\ of\ the\ ith\ element\ on\ the\ jth\ criterion$
- $W_j = the\ weight\ of\ the\ jth\ criterion$

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Apply What You Have Learned Today

- Next week you should:
  - Identify areas of complexity in your cyber environments
- In the first three months following this presentation you should:
  - Gain an understanding of how those complexities inhibit operations
  - Determine novel methods to measure degrees of complexity
- Within six months you should:
  - Establish bounds of operations and appetite that drive decisions for applying resources to reduce complexity
  - Utilize measures to drive risk-based decisions (i.e., cyber control selection)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You! – QUESTIONS?

Brett A. Tucker, PMP, CSSBB, CISSP, CGRC

batucker@cert.org

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.